Privacy Safeguards Program

WELCOME TO THE DEPARTMENT OF EDUCATION

The purpose of this document is to introduce you to ED's privacy safeguards program and your responsibilities for protecting the personal information that ED collects from millions of students, parents, grantees, employees, contractors and others.

In carrying out its mission ED must safeguard against an invasion of privacy through the misuse of records and allow the public to learn how their personal information is collected, maintained and used by the department.

What is ED's Privacy Safeguards Program?

The mission of ED's privacy safeguards program is to foster a culture of accountability throughout the ED community for the appropriate handling and protection of personal information. We do this through:

- Coordinating policy development and implementation across the department;
- Providing employee outreach and training;
- Providing technical guidance to program officials;
- Working closely with the office of the chief information officer to integrate safeguards for data protection and system security; and
- Participating in government-wide adoption of best practices.

ED's privacy safeguards program is carried out by the Records Management and Privacy Division of the Office of Management (OM), Regulatory Information Management Services (RIMS).

Who Has Access To Personal Information?

Many ED employees and contractors have access to personal information. You are allowed access only if you have an official need for the information. For example, human resources specialists and supervisors process personnel actions and are permitted to access personnel files. Other employees and contractors administer information systems that collect and use personal information collected from students, parents, grantees and others.

What Information Should I Protect?

You must protect the personal information collected, maintained and used by ED. Specifically, you must protect public, employee and contractor information that can be used to identify a particular person. Examples follow on the next page. This includes information in all forms – electronic, paper, verbal and other.

Privacy Safeguards Program

How Do I Report Privacy Incidents?

You must immediately report all actual or suspected incidents involving the loss, misuse or theft of personal information to your supervisor and your office's computer security officer (CSO). Within one hour, the CSO must notify ED's Chief Information Security Officer (CISO), who must report the incident to a government-wide incident response center.

Are There Penalties if I Do Not Safeguard Personal Information, or if I Do Not Report an Incident?

Yes. If an ED employee or contractor violates data privacy or system security requirements, he or she could face disciplinary, monetary and/or criminal penalties for each violation.

Penalties may also apply to the supervisor and the department.

What Are My Privacy Safeguards Responsibilities?

- Take your training. Everyone must take privacy awareness training once a year. There is also specialized training for system managers, program managers, and senior officials.
- Understand what information you are allowed to access. ED collects and maintains many types of personal data in various forms and at many locations. Talk with your supervisor about the access, if any, your work requires and what you may and may not do with the information.
- Keep information secure. Lock your workstation (CTRL + ALT+ DEL) when away from your desk and lock up files at the end of the day. Do not share your workstation password with anyone.
- Never include personal information within e-mail message text. Names, SSNs, dates of birth, etc., may be emailed only if contained in a password-protected attachment, or if the email is encrypted.
- Get rid of information you no longer need and are not required to keep. Shred paper documents, destroy CDs and DVDs, and delete information from your computer unless required to maintain by a records schedule, litigation hold, or outstanding record request.
- Be careful when traveling or telecommuting. Take only the information you need, do not keep your passwords with your computer or laptop, use a cable lock with your laptop, and always know where your laptop is and keep it safe.
- Report privacy and security incidents immediately. This includes accidental incidents such as information left on a copier at the end of the day, and malicious incidents, such as the theft of a laptop.

Examples of Personal Information

- Name
- Date and place of birth
- Social Security number
- Mother's maiden name
- Account numbers
- Financial, credit, education, medical data
- Telephone numbers
- Driver's license number
- Mailing address, E-mail addresses
- Dependent information
- Student loan record, file or case numbers
- Performance ratings
- Photograph
- Biometrics (fingerprint, iris scan)
- Any other unique identifying number, characteristic, or code derived from or related to information about the individual or otherwise capable of being used to identify the individual.

FOR MORE INFORMATION:
Privacy Safeguards Help Desk ▪ Phone: (202) 401-1269 ▪ E-mail: privacyadvocate@ed.gov
Dianne Novick, ED's Privacy Advocate ▪ (202) 401-8524